О Т З Ы В

на автореферат диссертации

Ахметзяновой Лилии Руслановны

«Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации», представленной на соискание ученой степени кандидата физико-математических наук по специальности 05.13.19 - «*Методы и системы защиты информации, информационная безопасность*»

Диссертационная работа Ахметзяновой Л.Р. посвящена решению важной задачи – разработке алгоритмических схем, обеспечивающих информационную безопасность систем защиты информации относительно свойств конфиденциальности и целостности передаваемых данных. Это так называемые AEAD-схемы – аутентифицированное шифрование с ассоциированными данными. Рассматриваемая задача имеет существенную практическую значимость в силу широкого использования AEAD-схем в системах защиты информации.

Исследования AEAD-схем выполняются в диссертационной работе в духе известного подхода к *доказательной* оценке стойкости алгоритмов защиты информации. В рамках исследований задаются формальные модели безопасности, включающие определения свойств, которые должны обеспечиваться анализируемой схемой, а также перечень возможностей, используемых противником для атаки на схему. Большинство AEAD-схем предполагает использование блочного симметричного алгоритма (БСА), к примеру, алгоритма из состава ГОСТ 34.12-2018. Обычно, в рамках доказательства стойкости AEAD-схемы, показывается, что из существования противника, успешно нарушающего какое-либо из свойств безопасности, обеспечиваемого AEAD-схемой, следует существование противника, обладающего эффективным методом анализа используемого БСА. Иными словами, выполняется так называемое *сведение* — стойкость AEAD-схемы сводится к стойкости БСА.

В диссертационной работе рассматриваются AEAD-схемы, где вместо БСА используется случайно выбранная секретная подстановка, при этом основное

внимание уделяется комбинаторным свойствам анализируемой схемы. Такое представление удобно, поскольку, с одной стороны, упрощаются математические выкладки, а с другой, при стандартном переходе от БСА к случайной подстановке, имеется возможность эвристически учесть результаты анализа конкретного БСА.

Существование *сведения* стойкости AEAD-схемы к стойкости БСА, во-первых, позволяет говорить о возможности применения AEAD-схемы на практике (при условии использования стойкого БСА). Во-вторых, результатом *сведения* является оценка сверху на преобладание противника, которое либо точно равно вероятности нарушения некоторого свойства безопасности, либо приближенно равно такой вероятности при переходе в более слабую модель безопасности. Верхняя оценка преобладания функционально зависит (в том числе) от количества обрабатываемых сообщений и блоков и, следовательно, позволяет дать обоснованное ограничение на объем обрабатываемых данных без смены предварительно распределенной секретной информации, т.е. решить актуальную практическую задачу, возникающую при исследовании свойств безопасности средств защиты информации.

Оценки преобладания, представленные в диссертационной работе, получены для «стандартных» моделей нарушителя: модели IND-CPA, определяющей свойство неотличимости в условиях адаптивно выбираемых открытых текстов, и модели INT-CTXT, определяющей свойство целостности шифртекстов. Кроме этого, оценки преобладания получены также для моделей, которые предполагают наличие у противника дополнительных возможностей, например, для модели MRAE-int, определяющей свойство целостности при возможности навязывания одинаковых синхропосылок. Результаты, полученные в моделях с дополнительными возможностями, позволяют говорить об устойчивости AEAD-схемы в условиях её некорректного применения, а также при сбоях в работе системы защиты информации, что ещё раз подчёркивает практическую важность представленного диссертационного исследования.

Следует отдельно выделить следующие полученные в диссертации результаты.

1. Разработана AEAD-схема MGM2, отличающаяся от оригинальной схемы

MGM двумя изменениями: 1) синхропосылка не шифруется, 2) устанавливается дополнительный флаг перед формированием имитовставки. Внесённые изменения позволяют: во-первых, улучшить эксплуатационные характеристики схемы, поскольку требуется на две операции шифрования меньше; во-вторых, существенно упростить доказательства стойкости в стандартных моделях свойств конфиденциальности и целостности; в-третьих, обосновать стойкость схемы в моделях угроз, где противнику предоставляются дополнительные возможности.

2. Разработаны схемы OMAC-ACPKM-Master и GCM-ACPKM, которые являются модификациями стандартизированных схем OMAC и GCM соответственно. Модификация заключается во внедрении «механизма внутреннего преобразования секрета» – ACPKM. Были получены оценки стойкости, демонстрирующие то, что внедрение упомянутого механизма позволяет обрабатывать сообщения многократно большей длины при сохранении заданного уровня стойкости.

3. Разработан метод нарушения свойства целостности AEAD-схемы «8 бит», являющейся композицией режима обеспечения конфиденциальности CTR и режима выработки имитовставки OMAC. Как следствие, получена оценка снизу на преобладание противника. Метод основан на использовании парадокса дней рождения.

4. Для AEAD-схемы MGM получены верхние оценки на преобладание противника в модели IND-CPA (конфиденциальность). Этот результат, в совокупности с аналогичным результатом в модели INT-CTXT (целостность), позволяет говорить о том, что MGM обеспечивает уровень стойкости, сопоставимый с таковым у других стандартизированных AEAD-схем.

Тема исследований диссертационной работы соответствует паспорту специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Автореферат диссертации структурирован, а также позволяет сделать вывод о научной новизне, теоретической и практической значимости диссертационного исследования. Автором подготовлено и опубликовано по теме диссертации 5 статей, из них 3 – в рецензируемых изданиях, рекомендованных для защиты в диссертационном совете МГУ по

специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Считаю, что диссертация Ахметзяновой Лилии Руслановны «Комбинаторные свойства схем обеспечения конфиденциальности и целостности информации» отвечает всем требованиям к кандидатским диссертациям, изложенным в «Положении о присуждении ученых степеней в Московском государственном университете имени М.В. Ломоносова», а ее автор, Ахметзянова Лилия Руслановна, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Кандидат физико-математических наук,
(старший специалист, ООО «СФБ Лаб») [redacted] И.М. Арбеков

Контактные данные:

тел.: [redacted], e-mail: igor.arbekov@sfblaboratory.ru

Адрес места работы:

127273, Москва, ул. Отрадная, д. 2Б, стр. 1, тел: +7 495 645 44 38

Я, Арбеков Игорь Михайлович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку. [redacted] «12» мая 2022 г.

Подпись Арбекова И.М. удостоверяю [redacted]

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
ООО «СФБ ЛАБ»
ЗАЛУНИН О.А.